WHAT IS CLAIMED IS:

1. A transceiver comprising:

a transmitter configured to transmit data signals;

a receiver configured to receive data signals; and

a controller configured to encrypt a string and supply the encrypted string to authenticate the transceiver.

2. The transceiver of claim 1, wherein the controller is configured to encrypt the string with a transceiver private encryption key.

3. The transceiver of claim 1, wherein the controller is configured to use a transceiver private encryption key and a transceiver public encryption key to authenticate the transceiver.

4. The transceiver of claim 3, wherein the controller is configured to encrypt the string with the transceiver private encryption key.

5. The transceiver of claim 3, wherein the transceiver public encryption key is sealed by encrypting the transceiver public encryption key with a system private encryption key and stored as a sealed transceiver public encryption key.

6. The transceiver of claim 5, wherein the sealed transceiver public encryption key is decrypted with a system public encryption key to retrieve the transceiver public encryption key.

7. The transceiver of claim 1, wherein the controller comprises an electrically erasable and programmable read only memory that is used to store a transceiver private encryption key and a transceiver public encryption key.

8. The transceiver of claim 1, wherein the controller comprises a cryptography module for encrypting the string.

9. The transceiver of claim 1, wherein the controller comprises an RSA encryption module for encrypting the string.

10. The transceiver of claim 1, wherein the receiver comprises a fiber optic receiver.

11. The transceiver of claim 1, wherein the transmitter comprises a fiber optic transmitter.

12. The transceiver of claim 1, wherein the transceiver comprises a small form factor pluggable transceiver.

13. A network system comprising:

a host;

an interface electrically coupled to the host; and

a transceiver comprising:

a transmitter configured to transmit data signals;

a receiver configured to receive data signals; and

a controller configured to communicate with the host through the interface to authenticate the transceiver with the host.

14. The network system of claim 13, wherein the interface comprises an inter-integrated circuit bus.

15. The network system of claim 13, wherein the interface comprises a transceiver fault status line.

16. The network system of claim 13, wherein the interface comprises a transceiver disable line.

17. The network system of claim 13, wherein the interface comprises a transmit data in line and an inverted transmit data in line.

18. The network system of claim 13, wherein the interface comprises a received data out line and an inverted received data out line.

19. The network system of claim 13, wherein the interface comprises a loss of signal status line.

20. The network system of claim 13, wherein the host is one of a mainframe computer, a workstation, a server, and a storage device.

21. The network system of claim 13, wherein the host is one of a bridge, a router, a hub, a local area switch and a wide area switch.

22. A transceiver comprising:

a transmitter configured to transmit data signals;

a receiver configured to receive data signals; and

a controller configured to communicate with a host to authenticate the transceiver with the host, wherein the controller comprises a first public key/private key pair for authentication.

23. The transceiver of claim 22, wherein the first public key/private key pair is associated with a first access code and the controller comprises a second public key/private key pair for authentication, wherein the second public key/private key pair is associated with a second access code.

24. The transceiver of claim 23, wherein the first public key/private key pair is used for authentication in response to the host communicating the first access code to the controller and the second public key/private key pair is used for authentication in response to the host communicating the second access code to the controller.

25. A fiber optic transceiver comprising:
means for transmitting data signals;
means for receiving data signals; and
means for authenticating the fiber optic transceiver upon installation of the fiber optic transceiver.

26. The fiber optic transceiver of claim 25, wherein the means for receiving data signals comprises means for converting optical serial data into electrical serial data.

27. The fiber optic transceiver of claim 25, wherein the means for transmitting data signals comprises means for converting electrical serial data into optical serial data.

28. The fiber optic transceiver of claim 25, wherein the means for authenticating the fiber optic transceiver comprises means for encrypting an authentication string using a transceiver specific private key, the encrypted authentication string configured to be decrypted using a transceiver specific public key.

29. A method for authenticating a transceiver in a system, comprising:
installing a transceiver in the system;
sending an authentication signal from the transceiver to a host;
analyzing the authentication signal in the host; and

selecting one of accepting and rejecting the transceiver based upon the analysis of the authentication signal.

30. The method of claim 29, wherein the authentication signal comprises a certificate identification.

31. The method of claim 29, wherein analyzing the authentication signal comprises decrypting the authentication signal using a public key of an issuing authority.

32. A method for authenticating a transceiver, comprising:

installing a transceiver comprising a transceiver specific public key/private key pair, wherein the transceiver specific public key is encrypted with a private key of an issuing authority;

requesting the encrypted transceiver specific public key from the transceiver;

passing the encrypted transceiver specific public key from the transceiver to a host; and

decrypting the encrypted transceiver specific public key in the host using a corresponding public key of the issuing authority to obtain the transceiver specific public key.

33. The method of claim 32 comprising:

generating an original authentication string in the host;

sending the original authentication string from the host to the transceiver;

encrypting the original authentication string in the transceiver using the transceiver specific private key;

passing the encrypted authentication string from the transceiver to the host; and

decrypting the encrypted authentication string in the host using the transceiver specific public key.

34. The method of claim 33 comprising:

comparing the decrypted authentication string to the original authentication string; and

selecting one of rejecting and accepting the transceiver based upon the comparison.

35. The method of claim 33, wherein the original authentication string is a random number.